International Journal of Pure and Applied Mathematics

Volume 18 No. 1 2005, 17-47

BILINEAR MULTIPLICATIONS IN $\mathbb{R}^n$ PART I. MULTIPLICATIONS, FINITE QUASIGROUPS AND BILINEAR MULTIPLICATIONS IN $\mathbb{R}^n$

Jan Rogulski

University for Economics Activities
Ul. Łabiszyńska, 03-204 Warsaw, POLAND
e-mail: mrogul@ibmer.waw.pl

Abstract: The bilinear multiplication $*$ in $\mathbb{R}^n$ is a bilinear mapping $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$. If it is associative, then $(\mathbb{R}^n, +, *)$ becomes a ring. Some of bilinear multiplications are induced by multiplications defined on a basis of $\mathbb{R}^n$. This is the reason why we first study the multiplications in finite sets. A multiplication $*$ in a set is called a quasigroup multiplication if its left and right multiplications are bijections and $*$ has a neutral element ($*$ need not be associative). Thus an associative quasigroup is a group. We give here the description of isomorphism classes of n-element quasigroups for $n = 2, 3, 4$ and 5 and examples for $n = 6$. In this first part of the study of bilinear multiplications in $\mathbb{R}^n$ we give several examples and we show that the complex numbers multiplication is not induced by any multiplication in any basis of $\mathbb{R}^2$. The quaternion multiplication also is not induced by any multiplication in any basis of $\mathbb{R}^4$. For general multiplications we explain the independence of such properties as commutativity, associativity, and possessing a unit-element.

Received: June 8, 2004

The forthcoming second part is devoted to spectral properties of bilinear multiplications, while the third deals with powers defined by non-associative multiplications.

AMS Subject Classification: 08A05, 17A01, 20N02
Key Words: non-associative multiplications, quasigroups non-associative rings, groupoids, binary operations

1. Independence of Commutativity, Associativity and the Existence of Unit-Element

Let X by any nonempty set. If X is finite then $\#X$ is the number of elements of X, $\#X \in \mathbb{N}$, otherwise $\#X := \infty$. We call any mapping $* : X \times X \to X$ defined on the whole $X \times X$ a multiplication in the set X. Such a map $* \in X^{X \times X}$ is sometimes called a binary operation in X with values in X (see Cohn [1] p. 40). Thus, if $\#X = n \in \mathbb{N}$ then there is $n^{(n^2)}$ distinct multiplications in X. By $x * y$ is denoted the value of $*$ corresponding to the pair $(x, y) \in X \times X$. A multiplication $*$ is said to be *commutative* if for every $(x, y) \in X \times X$ we have $x * y = y * x$. A multiplication $*$ is *associative* iff for each triple $(x, y, z) \in X^3$ the following equality holds

$$x * (y * z) = (x * y) * z.$$

An element $x \in X$ is a *left neutral element of* $*$ iff for every $\alpha \in X$ we have $x * \alpha = \alpha$. Similarly, an element y is a right neutral element iff for every $\alpha \in X$ the equality $\alpha * y = \alpha$ holds. An element $x \in X$ is called the *unit-element of* $*$ iff x is simultaneously left and right neutral element, i.e., $\alpha * x = x * \alpha = \alpha$ for every $\alpha \in X$.

1.1. Examples

1.1.1. If $\#X = 1$ then there is only one multiplication in X.

This multiplication is commutative, associative and the element of X is the unit-element of this multiplication.

1.1.2. Let X has at least two distinct elements and y let be anyone of them. Define

$$\alpha * \beta := y \quad \text{for every } (\alpha, \beta) \in X \times X.$$

This multiplication is clearly associative, commutative, and has neither left nor right neutral elements. If $x \in X$ and $x \neq y$ then $x * x = y$. Thus x is neither left nor right neutral element of $*$. Since $x * y = y \neq x$, we see that y is not a right neutral element of $*$. Also $y * x = y \neq x$. Therefore, y is not a left neutral element. Hence, every element of X is neither a left nor a right neutral element of $*$. Since y was chosen arbitrarily, we see that if $\#X \geq 2$ then there exist at least $\#X$ multiplications that are commutative and associative but have no any neutral element.

1.1.3. We now define a multiplication $*$ by the equality $\alpha * \beta := \beta$ that holds for every $(\alpha, \beta) \in X^2$, and we assume that $\#X \geq 2$. Then every element of X is a left neutral element of $*$. Since for any $y \in X$ and $\alpha \in X \setminus \{y\}$ we have $\alpha * y = y \neq \alpha$ then $*$ has no any right neutral element.

For every $(\alpha, \beta, \gamma) \in X^3$ we have

$$\alpha * (\beta * \gamma) = \alpha * \gamma = \gamma$$

and

$$(\alpha * \beta) * \gamma = \beta * \gamma = \gamma.$$

Thus, this multiplication is associative.

If $(x, y) \in X^2$ anf $x \neq y$ then $x * y = y$ while $y * x = x \neq x * y$. Therefore, $*$ is not commutative.

1.1.4. Similarly as above, if $\#X \geq 2$ and

$$\alpha * \beta := \alpha \quad \text{for every } (\alpha, \beta) \in X^2\,,$$

then this multiplication is associative and non-commutative, and every element of X is a right neutral element of $*$ while there is not any left neutral element of this multiplication.

1.1.5. The subsequent multiplication is defined by a fixed $x \in X$ as follows.

$$\alpha * \beta := \begin{cases} \beta & \text{if } \alpha = x, \\ \alpha & \text{if } \beta = x, \\ x & \text{otherwise.} \end{cases}$$

Then x is the unique unit-element of $*$. This multiplication defines a group structure on X if and only if $\#X \leq 2$. If $\#X \geq 3$ then $*$ is clearly commutative but it is not associative. For $y \in X,\ z \in X$ such that $y \neq x,\ z \neq x$ and $y \neq z$, we have

$$y * (y * z) = y * x = y,$$

while

$$(y * y) * z = x * z = z.$$

Every element α has an inverse element (not unique, if $\#X \geq 3$ and $\alpha \neq x$).

1.1.6. Fix an element $x \in X$ and then define:

$$\alpha * \beta = \begin{cases} \beta & \text{if } \beta \neq x, \\ \alpha & \text{if } \beta = x. \end{cases}$$

Obviously, x is the the unit-element of the multiplication $*$.

If $\#X \geq 2$ and $\alpha \in X \setminus \{x\}$ then $\alpha * x = \alpha \neq x$. Therefore, α is not a left neutral element, and hence α is not a unit-element. Also $x * \alpha = \alpha \neq x$, and thus α is not a right neutral element. The verification of associativity for this multiplication is a simple exercise. If $\#X \geq 2$ then $*$ is not a group structure on X, since for $\beta \neq x$ and for every $\alpha \in X$ we have $\alpha * \beta = \beta \neq x$, and hence β has no an inverse element.

Moreover, if $\#X \geq 3$ then $*$ is not commutative. One can see that for $y \in X$ and $z \in X$ such that $y \neq x$, $x \neq z$ and $y \neq z$ we have

$$y * z = z \neq y = z * y.$$

When $\#X = 2$ the multiplication defined in this example is commutative.

1.1.7. Let $X = \{x, y, z\}$. We define a multiplication in X by the following table

$*$	x	y	z
x	x	y	z
y	y	x	x
z	z	z	x

In the left column we have values of α, in the upper head-row stand values of β and the value $\alpha * \beta$ lies in the same row as α and in the same column as β. Then x is the unique unit-element of $*$, and this multiplication is not commutative. Nevertheless, every element of X has at least one left inverse element (for y it is only y, while for z the both elements y and z are left inverse elements). Every element of X has at least one right inverse element (y and z are right inverse elements for y and z is the unique right inverse element for z). Every element $\alpha \in X$ has unique element $\beta \in X$ such that $\alpha * \beta = \beta * \alpha = x$, i.e., β is simultaneously left and right inverse element of α, $\beta = \alpha^{-1}$. In fact, $\alpha^{-1} = \alpha$. But this multiplication is not a group structure, since $*$ is not associative:

$$y * (z * y) = y * z = x,$$

while

$$(y * z) * y = x * y = y.$$

In every set $\widetilde{X}$ such that $\#\widetilde{X} \geq 3$ a multiplication with the above properties can be defined. Consider $\widetilde{X} \supset X$ and let us extend $*$ onto $\widetilde{X} \times \widetilde{X}$ in the following manner

$$\begin{array}{ll} \alpha \,\widetilde{*}\, \beta = \alpha * \beta & \text{if } (\alpha,\beta) \in X \times X, \\ x \,\widetilde{*}\, \beta = \beta \,\widetilde{*}\, x = \beta & \text{for every } \beta \in \widetilde{X}, \\ \beta \,\widetilde{*}\, \beta = x & \text{for every } \beta \in \widetilde{X}, \\ \alpha \,\widetilde{*}\, \beta = y & \text{if } (\alpha,\beta) \in \widetilde{X} \times \widetilde{X} \setminus X \times X \text{ and } \alpha \neq \beta \\ & \text{and } \alpha \neq x \text{ and } \beta \neq x. \end{array}$$

The multiplication $\widetilde{*}$ is not commutative and it is not associative. Nevertheless, x is the unique unit-element of $\widetilde{*}$ and for every β we have $\beta^{-1} = \beta$.

1.1.8. For a set X such that $\#X \geq 2$, we first choose two distinct elements in X, say x and y, and next we define a multiplication in X as follows.

$$\alpha * \beta := \begin{cases} \beta & \text{if } \alpha = x, \\ \alpha & \text{if } \beta = x, \\ y & \text{if } \alpha \neq x \text{ and } \beta \neq x. \end{cases}$$

Obviously, this multiplication is commutative and the element x is the unit-element. If in a triple $(\alpha, \beta, \gamma) \in X^3$ at least one element is equal to x, we have

$$x * (\beta * \gamma) = \beta * \gamma = (x * \beta) * \gamma\,, \quad \alpha * (x * \gamma) = \alpha * \gamma = (\alpha * x) * \gamma\,,$$

$$\alpha * (\beta * x) = \alpha * \beta = (\alpha * \beta) * x.$$

Otherwise, i.e. if $\alpha \neq x,\ \beta \neq x$ and $\gamma \neq x$, we have

$$(\alpha * \beta) * \gamma = y * \gamma = y$$

and

$$\alpha * (\beta * \gamma) = \alpha * y = y.$$

Therefore, this multiplication is also associative. We conclude that $*$ is an associative and commutative multiplication with the unique unit-element. Nevertheless, it is not a group structure, since every $\alpha \in X \setminus \{x\}$ has no inverse element.

1.1.9. If $\#X \geq 2$, $(x, y) \in X \times X$ is fixed so that $x \neq y$, then the multiplication defined below

$$\alpha * \beta := \begin{cases} y & \text{if } (\alpha,\beta) = (x,x), \\ x & \text{if } (\alpha,\beta) \in X \times X \setminus \{(x,x)\} \end{cases}$$

is commutative and non-associative:

$$(x * x) * y = y * y = x, \qquad x * (x * y) = x * x = y$$

and for $(\alpha, \beta) \in X^2$ and $\alpha \neq \beta$ we have $\alpha * \beta = x = \beta * \alpha$. This multiplication has neither left nor right neutral element, since $x * x = y \neq x$ (and thus x is not a neutral element), and if $\alpha \neq x$ then $\alpha * \alpha = x \neq \alpha$, what means, that α also is not a neutral element.

1.1.10. Let X, x and y be as in 1.1.9. but the multiplication is now defined to be

$$\alpha * \beta := \begin{cases} y & \text{if } \alpha = x, \\ x & \text{if } \alpha \neq x. \end{cases}$$

Then

$$x = y * x = (x * y) * x \neq x * (y * x) = x * x = y$$

and

$$x = y * x \neq x * y = y.$$

Therefore, the multiplication $*$ is neither associative nor commutative. There exist no neutral element for this multiplication.

1.1.11. For X, x and y as in 1.1.9 and 1.1.10 we now define a multiplication $*$ is X by the formula

$$\alpha * \beta := \begin{cases} x & \text{if } \alpha \neq y, \\ y & \text{if } \alpha = y. \end{cases}$$

We see that for every $(\alpha, \beta, \gamma) \in X^3$ the following equalities hold. If $\alpha \neq y$ then

$$(\alpha * \beta) * \gamma = x * \gamma = x \quad \text{and} \quad \alpha * (\beta * \gamma) = x.$$

For $\alpha = y$ we obtain

$$(y * \beta) * \gamma = y * \gamma = y \quad \text{and} \quad y * (\beta * \gamma) = y.$$

Therefore, $*$ is an associative multiplication. Since

$$y = y * x \neq x * y = x,$$

we see that this multiplication is not commutative. When $\#X$=2, we have both x and y as right neutral elements and none of elements of X is a left neutral element. But if $\#X \geq 3$ then the multiplication defined here has neither left nor right neutral element.

1.1.12. Let X, x and y be as in previous three examples and

$$\alpha * \beta := \begin{cases} \beta & \text{if } \alpha = x, \\ x & \text{if } \alpha \neq x. \end{cases}$$

Clearly, the element x is the unique left neutral element and there exist no right neutral element, since $y * \beta = x \neq y$ for every $\beta \in X$. Since

$$y * (x * y) = x \quad \text{and} \quad (y * x) * y = x * y = y,$$

the multiplication $*$ is not associative. This multiplication is also not commutative, because

$$x * y = y \neq x = y * x.$$

Here the left neutral element is unique but $*$ has no unit-element.

1.1.13. Analogously as in the previous example we define a multiplication in X which is neither commutative nor associative and has exactly one right neutral element. It has not any left neutral element and thus $*$ also has not the unit-element. Namely,

$$\alpha * \beta = \begin{cases} \alpha & \text{if } \beta = x, \\ x & \text{if } \beta \neq x. \end{cases}$$

Then $(y*x)*y = x$ and $y*(x*y) = y*x = y$. Moreover, $y*x = y \neq x = x*y$.

The examples presented above prove the following theorem.

Theorem 1.2. *Let X be a set with $\#X \geq 3$. Then for every of eight configurations of properties: commutative or non-commutative, associative or non-associative, has a unit-element or not, there exists a multiplication $*$ in X with the desired triple of properties.*

To facilitate a review of Examples 1.1 proving Theorem 1.2 we write down the suitable table.

associativity	+	+	+	+	+	+	−	−	−	−	−	−
commutativity	+	+	−	−	−	−	+	+	−	−	−	−
unit-element	+	−	+	−	−	−	+	−	+	−	−	−
left neutral el.	+	−	+	+	−	−	+	−	+	−	+	−
right neutral el.	+	−	+	−	+	−	+	−	+	−	−	+
n s.t. $\#X \geq n$	1	2	3	2	2	3	3	2	3	2	2	2
t of Example 1.1.t	1,8	2	6	3	4	11	5	9	7	10	12	13

The sign + means that $*$ has this property and minus stands to indicate that $*$ has not this property. The table produced above contains all possible configurations of entries + and −.

It is obvious that the existence of unit-element means simultaneously the existence of a left neutral element and a right neutral element. We now prove the converse statement.

Proposition 1.3. *Let $*$ be a multiplication in $X, x \in X$ is a left neutral element of x and y is a right neutral element of $*$. Then $x = y$ and for every element $\alpha \in X \setminus \{x\}$ the element α is neither left nor a right neutral element.*

Proof. Since x is a left neutral element, we have $x * y = y$. On the other hand, since y is a right neutral element then $x * y = x$. Therefore, $x = y$. If $\alpha \in X$ and $\alpha \neq x$ (in particular, $\#X$ must satisfy inequality $\#X \geq 2$) then $x * \alpha = \alpha \neq x$ and hence α is not a right neutral element. Also $\alpha * x = \alpha \neq x$. This, in turn, means that α is not a left neutral element. □

The result proved above is a generalization of the uniqueness of a neutral element in a manoid (see Cohn [1] p. 40) and also implies the statement that a unit-element of any binary operation if it exists then it is unique (see Cohn [1], p. 43, Exercise (12)). It is also clear that if $*$ is commutative then a left neutral element is also a right neutral element and thus (if it exists) it is actually the unit-element.

Hence, we can conclude that the table presented in the proof of Theorem 1.2 is complete indeed. This table shows that some multiplications constructed in Examples 1.1 have the required configuration of properties for $\#X \geq 3$. We will show below that this restrictions cannot be weakened and that, in fact, when we have $\#X \geq 3$ in the table then for such configuration of properties there is no multiplication in a two-element set with these properties.

We provide now a complete list of 16 multiplications in a two-element set $X = \{x, y\}$. The standard names of multiplications for the case of $x =$ True and $y =$ False are written in the head-row.

α	β							$\Rightarrow$		$\Leftarrow$				OR	AND	$\Leftrightarrow$	XOR
x	x	y	y	x	x	y	y	x	y	x	y	x	y	x	x	x	y
x	y	y	x	x	y	x	y	y	y	x	x	x	y	x	y	y	x
y	x	x	y	y	x	x	y	x	x	y	y	x	y	x	y	y	x
y	y	x	x	y	y	x	x	x	y	x	y	x	y	y	y	x	y
	A	−	−	+	+	−	−	−	−	−	−	+	+	+	+	+	+
	C	−	−	−	−	+	+	−	−	−	−	+	+	+	+	+	+
	$\#_L$	0	0	0	2	0	0	1	1	0	0	0	0	1	1	1	1
	$\#_R$	0	0	2	0	0	0	0	0	1	1	0	0	1	1	1	1

$A =$ Associativity, $C =$ Commutativity,

$\#_L =$ the number of left neutral elements,
$\#_R =$ the number of right neutral elements.

Table 1.4: Classes of multiplications in $X = \{x, y\}$

In columns we have values $\alpha * \beta$ corresponding to the values of α and β listed in the first and the second column, respectively. For every multiplication defined in a single column we assign '+' in the associativity row if this multiplication is associative and '−' if it is not the case. Similarly, we indicate by '+' or '−' whether a multiplication is commutative or not.

Definition 1.5. We say that multiplications $*$ in X and $\circ$ in Y are equivalent (or isomorphic) iff there exists a bijection $\varphi : X \to Y$ such that for every $(\alpha, \beta) \in X \times X$ we have

$$\varphi(\alpha * \beta) = \varphi(\alpha) \circ \varphi(\beta).$$

When $X = \{x, y\} = Y$ we have exactly two bijections, namely, one of them is the identity mapping and the other is τ, where $\tau(x) = y$ and $\tau(y) = x$. Thus the equivalence classes of isomorphic multiplications consist of a single multiplication or of two multiplications. The vertical double-lines divide the set of multiplications listed in Table 1.4 into 10 classes of isomorphic multiplications.

Among 16 multiplications in $X = \{x, y\}$ we have two that are non-associative, non-commutative and have not any neutral element. They are not isomorphic, i.e., τ is an automorphism for each of them. Another two multiplications have 2 neutral elements for each of them and they are non-commutative and associative. They are not isomorphic each other (one has two left neutral elements and the second has two right neutral elements). Next two multiplications are non-associative and commutative, and both are equivalent. Such multiplications have no neutral element. Notice, that Example 1.1.5 shows for any X with $\#X \geq 3$ a non-associative and commutative multiplication with a unit-element. In our case of $X = \{x, y\}$, when $*$ is non-associative and non-commutative but it has a neutral element (left or right) then this element is unique. There are two equivalent such multiplications with a left neutral element and other two equivalent such multiplications with a right neutral element. There are also six commutative and associative multiplications which split into 3 equivalence classes. First contains 2 multiplications with a unit-element which are not group structures and the third one contains 2 multiplications which are group structures (both isomorphic to $(\{+1, -1\}, \cdot)$, where $\cdot$ is usual multiplication of integers).

Let us note also that if $\#X = 2$ and a multiplication $*$ has the unit-element then $*$ is commutative and associative. This is not the case when $\#X \geq 3$, as Examples 1.1.5–7 do show. Another fact is also noteworthy for $X = \{x, y\}$. Namely, every associative and non-commutative multiplication has two neutral elements — either both are right or both are left neutral elements. When $\#X \geq 3$ this may not be the case, as Example 1.1.11 does prove. The multiplications for the cases $\#X \geq 3$ constructed in this example have no any neutral element but they are associative and non-commutative.

Since for a commutative action the existence of a left (or right) neutral element is equivalent to the existence of the unique unity (see Proposition 1.3), we have 12 available configurations of possessing or not the following four properties: commutativity, associativity, the existence of a left neutral element and the existence of a right neutral element. If $\#X \geq 3$ then for every choice of a configuration of properties mentioned above there exists a multiplication possessing such properties. Thus these four properties (with the nstural constraint that for commutative cases either $*$ has the unit-element or has no any neutral element) are for every X with $\#X \geq 3$ completely independent. The assumption that $\#X \geq 3$ cannot be weakened, since in the case of $\#X = 2$ the existence of unit-element implies commutativity, and therefore these properties are not independent for multiplications in a two-element set.

2. Classes of Multiplications

Every multiplication $*$ in X defines its conjugate multiplication $\bar{*}$ as follows

$$\alpha \,\bar{*}\, \beta := \beta * \alpha \quad \text{for every } (\alpha, \beta) \in X^2.$$

Of course, $*$ and $\bar{*}$ need not be different. In fact, $* = \bar{*}$ if and only if $*$ is a commutative multiplication. The conjugacy mapping $X^{X\times X} \ni * \mapsto \bar{*} \in X^{X\times X}$ is idempotent, that is, $\overline{(\bar{*})} = *$ for every multiplication $*$ in X. If we define in $X^{X\times X}$ a conjugacy relation as follows

$$* \sim_c \circ \quad \text{if and only if} \quad * = \circ \quad \text{or} \quad \circ = \bar{*}$$

then this is an equivalence relation.

The space $X^{X\times X}/{\sim_c}$ of conjugacy classes has a lot of elements, since $[*] = \{*\}$ consists of a single element for a commutative multiplication $*$ and $[*] = \{*, \bar{*}\}$ has two elements for every non-commutative $*$. Thus, if $\#X = n$ then

$$\#(X^{X\times X}/{\sim_c}) = n^{n(n+1)/2} + \frac{1}{2}(n^{n^2} - n^{n(n+1)/2}) = \frac{1}{2}(n^{n^2} + n^{n(n+1)/2}).$$

On the other hand, we can split $X^{X\times X}$ into two classes by means of any of such properties as commutativity, associativity or possessing the unit-element. Using all of these properties together we can divide $X^{X\times X}$ (with $\#X \geq 3$) into 8 nonempty and pairwise disjoint subsets, one containing all associative, commutative multiplications with unit-element, other containing all non-associative, commutative multiplications with unit-element, and so on. For $\#X = 2$ these properties split the set of multiplications into 5 nonempty classes, since all multiplications with the unit-element are already commutative and associative (see 1.4). The conjugacy relation $\sim_c$ agrees with the equivalence relation defining classes described above (and is more fine) since $*$ is commutative iff $\bar{*}$ is, and $*$ is an associative multiplication iff $\bar{*}$ is, and also $*$ has the unit-element if and only if this element of X is the unit-element of $\bar{*}$.

Taking any bijection $\varphi : X \to X$ and a multiplication $* \in X^{X\times X}$, we can define another multiplication $*_\varphi$ in X by the formula

$$x *_\varphi y := \varphi^{-1}(\varphi(x) * \varphi(y)) \quad \text{for every } (x, y) \in X^2.$$

Then $*_\varphi$ and $*$ are isomorphic and $\circ$ is an isomorphic multiplication in X to $*$ if and only if there exists a bijection $\varphi : X \to X$ such that $\circ = *_\varphi$. Of course, if $\circ = *_\varphi$ then $* = \circ_\psi$ for $\psi = \varphi^{-1}$ and $* = *_\varphi$ for $\varphi = \mathrm{id}$ (φ is the identity mapping). Also, if $\square = *_\varphi$ and $\triangle = \square_\psi$ for bijections φ, ψ of X, then $\triangle = *_\eta$, where $\eta = \varphi \circ \psi$ (here $(\varphi \circ \psi)(x) = \varphi(\psi(x))$). Therefore, the relation $\sim$ in $X^{X\times X}$ defined as follows:

$$* \sim \square \text{ if and only if there exist a bijection } \varphi : X \to X$$

such that $\square = *_\varphi$, is an equivalence relation. When $\#X = n$ then there exist $n!$ bijections (permutations) on X. Therefore, a class of isomorphic multiplications consists in this case of at most $n!$ elements, and thus

$$\#(X^{X\times X}/\sim) \geq n^{n^2}/n!$$

For $n \geq 2$ the above inequality is always strict. If $n = 2$ then $\#(X^{X\times X}/\sim) = 10$, while $n^{n^2}/n! = 8$. The right action of the group $(Bij(X), \circ)$ of bijections of X onto the set $X^{X\times X}$ ($\#X > 1$) defined by

$$X^{X\times X} \ni * \mapsto *_\varphi \in X^{X\times X}$$

is not free. For $\#X = 2$ it is shown in Table 1.4. If $\#X \geq 3$ and $x \in X$ is fixed, then the stabilizer of $*$, where $\alpha * \beta = x$ for every $(\alpha, \beta) \in X^2$, consists of all bijections that have x as a fixed point (if $\#X = n \geq 3$ then this subgroup of $Bij(X)$ has $(n-1)!$ elements). Thus, $[*]$ has exactly n elements (constant mappings on $X \times X$ into X). Therefore, if $\#X > 1$ then

$$\#(X^{X\times X}/{\sim}) > n^{n^2}/n!\,. \tag{1}$$

This number is very large. For instance, if $\#X = 3$ then the number of classes of isomorphic multiplications is greater than $\frac{1}{2}3^8$. Since $n! \leq n^n$ for every natural number, we see that the number of classes of isomorphic multiplications exceeds $n^{n(n-1)}$.

Similarly as $\sim_c$ the relation $\sim$ also agrees with the relations defined by commutativity, associativity and the existence of the unity properties and is more fine than each of them. It is easy to check that $*$ is commutative iff $*_\varphi$ is. Also, $*$ is associative if and only if $*_\varphi$ is associative. Moreover, if $x \in X$ is the unit-element of $*$ then $\varphi^{-1}(x)$ is the unit-element of $*_\varphi$. But $\sim_c$ and $\sim$ does not agree. For instance, if $\#X = 2$ then $\Rightarrow$ and $\Leftarrow$ are conjugated (see Table 1.4), but they lie in different classes of isomorphic multiplications. On the other hand, if $*$ and $\Box$ are isomorphic ($\Box = *_\varphi$ for $\varphi \in Bij(X)$) then for every $(\alpha, \beta) \in X^2$ we have

$$\alpha \,\bar{\Box}\, \beta = \beta \,\Box\, \alpha = \varphi^{-1}(\varphi(\beta) * \varphi(\alpha)) = \varphi^{-1}(\varphi(\alpha) \,\bar{*}\, \varphi(\beta)) = \alpha (\bar{*})_\varphi \beta,$$

that is, $\bar{\Box}$ and $\bar{*}$ are also isomorphic.

Therefore, the conjugacy mapping

$$\text{Con} : X^{X\times X} \ni * \mapsto \bar{*} \in X^{X\times X}$$

projects to a mapping $\text{Con}_0 : X^{X\times X}/{\sim} \;\to X^{X\times X}/{\sim}$ such that the diagram

$$\begin{pmatrix} X^{X\times X} & \xrightarrow{\text{Con}} & X^{X\times X} \\ \downarrow & & \downarrow \\ X^{X\times X}/{\sim} & \xrightarrow{\text{Con}_0} & X^{X\times X}/{\sim} \end{pmatrix}$$

is commutative.

Namely, $\text{Con}_0([*]) = [\bar{*}]$. Again, Con_0 is an idempotent mapping and defines an equivalence relation $\sim_0$ on $X^{X\times X}/{\sim}$. For $\xi \in X^{X\times X}/{\sim}$ and $\eta \in X^{X\times X}/{\sim}$, we have

$$\xi \sim_0 \eta \text{ if and only if } \xi = \eta \text{ or } \eta = \text{Con}_0(\xi).$$

The multiplication structure is thus an element of $(X^{X\times X}/{\sim}) \sim_0$, where we identify simultaneously not only isomorphic multiplications (obtained by "re-naming" elements of X through $\varphi \in Bij(X)$), but also the system of writing either from the left to right or "arabic" is neglected.

For instance, if $X = \{x, y\}$ then the space $X^{X\times X}/\sim$ of 10 isomorphism classes of multiplications in X splits into 7 conjugacy classes, the elements of $(X^{X\times X}/\sim)/\sim_0)$. Only one of them contain an isomorphism class of group multiplications.

3. Quasigroups

In the case of $\#X = 3$ we also have the unique (in $X^{X\times X}/\sim$) isomorphism class of group multiplications in X. Every group multiplication $*$ in a three-element set X is isomorphic to the usual complex numbers multiplication in the set $\{1, \exp 2\pi i/3, \exp 4\pi i/3\} \subset \mathbb{C}$ of all third-order roots of 1.

When $\#X = 4$ there exist two isomorphism classes in $X^{X\times X}/\sim$ of group structures. Every group multiplication on X is isomorphic either to matrix multiplication in the set

$$X_1 = \left\{ \begin{bmatrix} 1, & 0 \\ 0, & 1 \end{bmatrix}, \begin{bmatrix} 1, & 0 \\ 0, & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0, & -1 \end{bmatrix}, \begin{bmatrix} -1, & 0 \\ 0, & 1 \end{bmatrix} \right\},$$

or to the multiplication of complex numbers in the set

$$X_2 = \{1, i, -1, -i\} \subset \mathbb{C}$$

of all fourth-order roots of 1.

While in the case of $\#X = 3$ we have 3^9 different multiplications and in the case of $\#X = 4$ there is 4^{16} different multiplications, nevertheless, all group multiplications in these cases are commutative. Moreover, if $\#X \leq 4$ then every multiplication $*$ in X such that the left multiplications

$$L_x : X \ni y \mapsto x * y \in X$$

and right multiplications

$$R_x : X \ni y \mapsto y * x \in X$$

are all bijections for every $x \in X$, is already a group multiplication, i.e., it is also associative (see Cohn [1], p. 44, Theorem 1, for the proof that this properties imply the existence and uniqueness of inverse elements). When $\#X = 3$ and $*$ has the unit-element, let us denote it by $\mathbb{1}$, and other elements by a and b, $X = \{\mathbb{1}, a, b\}$. Then the condition that L_x, R_x are bijections for every $x \in X$

gives the following result

$*$	$\mathbb{1}$	a	b
$\mathbb{1}$	$\mathbb{1}$	a	b
a	a	b	$\mathbb{1}$
b	b	$\mathbb{1}$	a

Thus, defining $\varphi(\mathbb{1}) = 1$, $\varphi(a) = z := \exp(2\pi i/3)$, $\varphi(b) = z^2$, we see that $(X, *)$ and $(\{1, z, z^2\}, \cdot)$ are isomorphic groups.

If $\#X = 4$ and a multiplication $*$ has the unit-element $\mathbb{1}$, we have two possibilities. When $x * x = \mathbb{1}$ for every $x \in X$ then the multiplication $*$ in $X = \{\mathbb{1}, a, b, c\}$ such that L_x, R_x are one-to-one for every $x \in X$, has the form.

$*$	$\mathbb{1}$	a	b	c
$\mathbb{1}$	$\mathbb{1}$	a	b	c
a	a	$\mathbb{1}$	c	b
b	b	c	$\mathbb{1}$	a
c	c	b	a	$\mathbb{1}$

There are exactly four such multiplications in X, and each of them is determined by the choice of an element in X to be the unit-element $\mathbb{1}$. Every such multiplication has $3! = 6$ automorphisms, and all four are isomorphic to the group of four matrices mentioned above:

$$\varphi(\mathbb{1}) := \begin{bmatrix} 1, & 0 \\ 0, & 1 \end{bmatrix}, \quad \varphi(a) := \begin{bmatrix} -1, & 0 \\ 0, & 1 \end{bmatrix},$$

$$\varphi(b) := \begin{bmatrix} 1, & 0 \\ 0, & -1 \end{bmatrix}, \quad \varphi(c) := \begin{bmatrix} -1, & 0 \\ 0, & -1 \end{bmatrix}.$$

When $\#X = 4$ and $*$ has unit-element $\mathbb{1}$ but there exists $a \in X$ such that $a * a \neq \mathbb{1}$, then assuming that every L_x and R_x is bijective, we get the following table of multiplication $*$.

$*$	$\mathbb{1}$	a	b	c
$\mathbb{1}$	$\mathbb{1}$	a	b	c
a	a	b	c	$\mathbb{1}$
b	b	c	$\mathbb{1}$	a
c	c	$\mathbb{1}$	a	$b.$

There exist $4 \cdot 3 = 12$ such multiplications, each one determined by the choice of an element to be the unit-element $\mathbb{1}$ and by the choice of an element different from the previous one to be b (such that there exists $y \in X$ for which $y * y = b \neq \mathbb{1}$). These 12 multiplications are mutually isomorphic each other and every of them is isomorphic to the usual complex number multiplication in the set $\{1, i, -1, -i\}$, $\psi(\mathbb{1}) = 1$, $\psi(a) := i$, $\psi(b) := -1$, $\psi(c) := -i$. Every such multiplication is a group multiplication with two automorphisms, the non-identical being φ, where $\varphi(\mathbb{1}) := \mathbb{1}$, $\varphi(a) := c$, $\varphi(c) := a$, $\varphi(b) := b$.

Definition 3.1. We call $(X, *)$ a quasigroup if and only if $*$ is a multiplication in a nonempty set X with the following two properties.

(i) There exists in X the unit-element of multiplication $*$.

(ii) For every $x \in X$ the left multiplication L_x and the right multiplication R_x are bijections.

We have just proved that if $\#X \leq 4$ then every quasigroup is a commutative group. However, this is not the case for any X with $\#X \geq 5$. For a five-element set X we have 6 isomorphism classes of quasigroups which can be represented by the following multiplications, non-isomorphic each other.

3.2. The Table of 5-Element Quasigroups

(i)

$\cdot$	$\mathbb{1}$	a	b	c	d
$\mathbb{1}$	$\mathbb{1}$	a	b	c	d
a	a	b	c	d	$\mathbb{1}$
b	b	c	d	$\mathbb{1}$	a
c	c	d	$\mathbb{1}$	a	b
d	d	$\mathbb{1}$	a	b	c

(ii)

0	$\mathbb{1}$	a	b	c	d
$\mathbb{1}$	$\mathbb{1}$	a	b	c	d
a	a	b	c	d	$\mathbb{1}$
b	b	d	a	$\mathbb{1}$	c
c	c	$\mathbb{1}$	d	a	b
d	d	c	$\mathbb{1}$	b	a

(iii)

$*$	$\mathbb{1}$	a	b	c	d
$\mathbb{1}$	$\mathbb{1}$	a	b	c	d
a	a	$\mathbb{1}$	c	d	b
b	b	d	a	$\mathbb{1}$	c
c	c	b	d	a	$\mathbb{1}$
d	d	c	$\mathbb{1}$	b	a

(iv)

$\square$	$\mathbb{1}$	a	b	c	d
$\mathbb{1}$	$\mathbb{1}$	a	b	c	d
a	a	$\mathbb{1}$	c	d	b
b	b	d	$\mathbb{1}$	a	c
c	c	b	d	$\mathbb{1}$	a
d	d	c	a	b	$\mathbb{1}$

(v)

$\triangle$	$\mathbb{1}$	a	b	c	d
$\mathbb{1}$	$\mathbb{1}$	a	b	c	d
a	a	$\mathbb{1}$	c	d	b
b	b	c	d	a	$\mathbb{1}$
c	c	d	$\mathbb{1}$	b	a
d	d	b	a	$\mathbb{1}$	c

(vi)

$\triangledown$	$\mathbb{1}$	a	b	c	d
$\mathbb{1}$	$\mathbb{1}$	a	b	c	d
a	a	$\mathbb{1}$	c	d	b
b	b	c	d	$\mathbb{1}$	a
c	c	d	a	b	$\mathbb{1}$
d	d	b	$\mathbb{1}$	a	c.

Only $(X, \cdot)$ from Table 3.2 is a group. This group is commutative. Moreover, every commutative 5-element quasigroup is a group. Every non-commutative multiplication in 5-element quasigroup is simultaneously non-associative. One can check by simple calculations that if we replace $\cdot$ in the equality

$$b \cdot (c \cdot d) = (b \cdot c) \cdot d$$

by $\circ$ or $*$ or $\square$ or $\triangle$ or $\triangledown$ then we obtain inequality.

But the situation rapidly changes for the case of $\#X \geq 6$. Then it is no longer true that every commutative quasigroup is a group. Also not every group is commutative. As it is well known, the set Sym_3 of 3-element permutations has $3! = 6$ elements and the composition $\circ$ of permutations is a non-commutative and associative group multiplication in $X = \mathrm{Sym}_3$.

Example 3.3. (Commutative Quasigroup) In the set $X = \{\mathbb{1}, a, b, c, d, e\}$ we define the multiplication $*$ by the table below.

$*$	$\mathbb{1}$	a	b	c	d	e
$\mathbb{1}$	$\mathbb{1}$	a	b	c	d	e
a	a	$\mathbb{1}$	c	d	e	b
b	b	c	$\mathbb{1}$	e	a	d
c	c	d	e	$\mathbb{1}$	b	a
d	d	e	a	b	$\mathbb{1}$	c
e	e	b	d	a	c	$\mathbb{1}$

We see that $(b * b) * c = \mathbb{1} * c = c$ while $b * (b * c) = b * e = d$. Hence, $*$ is non-associative and commutative quasigroup. Therefore, $(X, *)$ is not a group.

We have also two commutative group structures in a 6-element set. One of them can be represented by

$$X_1 = \{1, z, z^2, z^3, z^4, z^5\} \subset \mathbb{C}, \qquad z = \exp(2\pi i/3),$$

with usual complex numbers multiplication. It has single generator z of rank 6 (z^5 can also be taken as a single generator). The second one is isomorphic to a commutative group with two generators a and u with $a^3 = \mathbb{1}$ and $u^2 = \mathbb{1}$. Then

$$X_2 = \{1, a, a^2, u, au, a^2u\}.$$

If we denote $au =: v$, $a^2u =: w$ and $a^2 =: b$, we obtain the table of multiplication

$\times$ in X_2 as follows.

$\times$	$\mathbb{1}$	a	b	u	v	w
$\mathbb{1}$	$\mathbb{1}$	a	b	u	v	w
a	a	b	$\mathbb{1}$	v	w	u
b	b	$\mathbb{1}$	a	w	u	v
u	u	v	w	1	a	b
v	v	w	u	a	b	1
w	w	u	v	b	1	$a.$

The commutative group $(X_2, \times)$ is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_2 = \{1, -1\}$, $\mathbb{Z}_3 = \{1, c, c^2\}$, $c = \exp(2\pi i/3)$. The isomorphism $\varphi : (X, \times) \to (\mathbb{Z}_2 \times \mathbb{Z}_3, \cdot)$ may be defined by equalities $\varphi(a) = (1, \exp(2\pi i/3))$ and $\varphi(u) = (-1, 1)$ for generators a and u.

When $\#X = n > 2$ then the number of isomorphism classes of multiplications in X is very large (see (1)). For $n = 3$ it is bigger than $\frac{1}{2}3^8$ and we have among all classes (elements of $X^{X\times X}/\sim$) only one which is a quasigroup (in fact, a commutative group) structure. For $n = 4$ there exist more than $4^{16}/24$, i.e., more than $\frac{1}{3}2^{29}$ multiplication structures, while only two of them are quasigroup structures (they are commutative group structures). If $n = 5$ then the number of multiplication structures exceeds $5^{25}/120 > 5^{22}$. But only 6 of them are quasigroup structures and among them only one is commutative and this one is a group structure. Other 5 quasigroup structures are not group structures. They are neither commutative nor associative. The classification of quasigroups seems to be a challenging and difficult problem.

Every element of a quasigroup has unique left inverse element and has unique right inverse element. As we see from Table 3.2, they need not be equal. Example 3.3 does show that even if for every $x \in X$ both (left and right) inverse elements are equal then this property does not imply associativity of $*$. Obviously, for every commutative quasigroup multiplication both inverse elements of an element $x \in X$ are equal.

One can say that $(X, *)$ is a group if and only if $(X, *)$ is a quasigroup and $*$ is associative. The classification theory of finite group structures is already completed. We refer to Kurzweil, Stellmacher [2], Lubotzky, Segal [4] and Seress [5] for this theory and for further bibliography in this subject.

4. Bilinear Multiplications in $\mathbb{R}^n$

Clearly, every bilinear map $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ is a multiplication in $\mathbb{R}^n$. For every bilinear multiplication b and any fixed basis $\{z_1, \ldots, z_n\}$ in $\mathbb{R}^n$ there exist

n^3 real numbers b_{ij}^k, $i,j,k \in \{1,2,\ldots,n\}$, such that

$$b(z_i, z_j) = \sum_{k=1}^{n} b_{ij}^k z_k$$

and

$$b(x,y) = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} \sum_{j=1}^{n} b_{ij}^k \lambda_i \mu_j \right) z_k$$

for

$$x = \sum_{i=1}^{n} \lambda_i z_i \quad \text{and} \quad y = \sum_{j=1}^{n} \mu_j z_j.$$

The space of all bilinear maps in $\mathbb{R}^n$ with values in $\mathbb{R}^n$ is a real vector space (under the usual addition of vector valued functions and multipying them by scalars) of dimension n^3.

Suppose now that $*$ is a multiplication in a basis $\mathcal{Z} = \{z_1, \ldots, z_n\}$ of $\mathbb{R}^n$. Then we can define a multiplication $\times : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ by the formula:

$$x \times y := \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \mu_j z_i * z_j,$$

where $\lambda_i s$ and $\mu_j s$ are coordinates of a and y in the basis $\mathcal{Z}$, respectively. We then call $\times$ a *multiplication induced by the multiplication* $*$ in the basis $\mathcal{Z}$. The induced multiplication $\times$ is a bilinear multiplication in $\mathbb{R}^n$, since

$$x \times y = \sum_{i=1}^{n} \sum_{j=1}^{n} z_i^*(x) z_j^*(y) z_i * z_j \,,$$

where $\{z_1^*, \ldots, z_n^*\}$ is the dual basis in the space $(\mathbb{R}^n)^*$ of linear forms on $\mathbb{R}^n$ which is defined by the basis $\mathcal{Z}$.

In the case of $n = 1$ every non-zero bilinear multiplication is of the form above. If $b : \mathbb{R}^1 \times \mathbb{R}^1 \to \mathbb{R}^1$ is a non-zero bilinear map then there exists $\beta \in \mathbb{R} \setminus \{0\}$ such that $b(x,y) = \beta xy$. Taking $z_1 := \frac{1}{\beta}$ we see that

$$b(\lambda z_1, \mu z_1) = \beta \lambda z_1 \mu z_1 = \lambda\mu/\beta = \lambda\mu z_1,$$

i.e.,

$$b(x,y) = x \times y,$$

where $\mathcal{Z} = \{z_1\}$ and $z_1 * z_1 := z_1$ is the unique multiplication in the one-point set $\mathcal{Z}$. Thus we proved that if $n = 1$ then every non-zero bilinear multiplication is induced by the multiplication defined in a suitable basis $\mathcal{Z}$ of $\mathbb{R}^n$. But if $n > 1$ then this is not the case. The following example will explain this matter.

Example 4.1. Let $n \geq 2$ and

$$\pi_n : \mathbb{R}^n \ni (x_1, \ldots, x_n) \mapsto x_1 + ix_2 \in \mathbb{C}$$

is the projection on $\mathbb{R}^2$. Let us define

$$j : \mathbb{C} \ni x_1 + ix_2 \mapsto (x_1, x_2, 0, \ldots, 0) \in \mathbb{R}^n.$$

Then $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$, defined as follows

$$b(x, y) := j(\pi_n(x) \cdot \pi_n(y)),$$

where $\cdot$ denotes usual multiplication of complex numbers, is a bilinear map.

We will prove now the following lemma.

Lemma 4.2. *The bilinear multiplications defined in Example 4.1 are not induced by any multiplication in any basis of* $\mathbb{R}^n$.

Proof. We see that the image $b(\mathbb{R}^n \times \mathbb{R}^n) \subset \mathbb{C} \times \{0\}$, $0 \in \mathbb{R}^{n-2}$. Suppose now that there exists a basis $\mathcal{Z} = \{z_1, \ldots, z_n\} \subset \mathbb{R}^n$ and a multiplication $*$ in $\mathcal{Z}$ inducing b. Then for every $i, j \in \{1, \ldots, n\}$ we would have $b(z_i, z_j) = z_i * z_j \in \mathbb{C} \times \{0\}$. On the other hand $z_i * z_j \in \mathcal{Z}$. If there exists a unique $k \in \{1, \ldots, n\}$ such that $z_i * z_j = z_k$ for every $i, j \in \{1, \ldots, n\}$ then $z_k = (w, 0, \ldots, 0)$ for certain $w \in \mathbb{C}$ and $b(z_k, z_k) = (w^2, 0, \ldots, 0) = (w, 0, \ldots, 0)$. Hence, $w = 1$ and $z_k = (1, 0, \ldots, 0)$. If b was induced by this (constant) multiplication $*$ in $\mathcal{Z}$ then its image would be $\mathbb{R} \times \{0\}$, where $0 \in \mathbb{R}^{n-1}$, what is not the case, since $b((1, 0, \ldots, 0), (0, 1, 0, \ldots, 0)) = (0, 1, 0, \ldots, 0)$. Therefore there must exist two different indices k and l such that $z_i * z_j = z_k$ and $z_{i'} * z_{j'} = z_l$ and also $\{z_k, z_l\}$ spans $\mathbb{C} \times \{0\}$, $0 \in \mathbb{R}^{n-2}$. Thus $z_k = (w, 0)$, $z_l = (\zeta, 0)$, $0 \in \mathbb{R}^{n-2}$. We calculate by means of the definion of b

$$\begin{aligned}
&b(z_k, z_l) = b(z_l, z_k) = (w\zeta, 0), \\
&b(z_k, z_k) = (w^2, 0), \\
&b(z_l, z_l) = (\zeta^2, 0).
\end{aligned}$$

If we have $z_k * z_l = z_l$, then $w\zeta = \zeta$ and $w = 1 \in \mathbb{C}$. In this case, if $z_l * z_l = z_l$ then $\zeta^2 = \zeta$ and therefore $\zeta = 1 = w$ what contradicts that $\{w, \zeta\}$ spans $\mathbb{R}^2$. Hence, $z_l * z_l = z_k$, that is, $\zeta^2 = 1 \in \mathbb{C}$. Since $\zeta \neq w = (1, 0) \in \mathbb{R}^2$ we obtain $\zeta = (-1, 0) \in \mathbb{R}^2$. But now $\zeta = -w$, therefore $\{w, \zeta\}$ also does not span $\mathbb{R}^2$ in the case of $z_l * z_l = z_k$. This concludes the proof. $\square$

Every multiplication $m : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$, bilinear or not, can be uniquely decomposed into a sum

$$m = m_S + m_A,$$

where $m_S(x,y) = m_S(y,x)$ and $m_A(x,y) = -m_A(x,y)$ for every $(x,y) \in \mathbb{R}^n \times \mathbb{R}^n$, that is, m_S is a commutative multiplication, and m_A is skew. Then

$$\begin{aligned} m_S(x,y) &= \frac{1}{2}[m(x,y) + m(y,x)], \\ m_A(x,y) &= \frac{1}{2}[m(x,y) - m(y,x)], \end{aligned}$$

what may easily be derived from the system of equations

$$\begin{cases} m_S(x,y) + m_A(x,y) = m(x,y), \\ m_S(x,y) - m_A(x,y) = m(y,x). \end{cases}$$

If we additionally assume that m is bilinear then the function $f : \mathbb{R}^n \ni x \mapsto m(x,x) \in \mathbb{R}$ is sufficient to define m_S:

$$m_S(x,y) = \frac{1}{2}[f(x+y) - f(x) - f(y)], \qquad f(x) = m(x,x),$$

and

$$m_A(x,y) = m(x,y) - m_S(x,y).$$

If m is bilinear then multiplications m_S and m_A are bilinear.

The left multiplication $L_x : \mathbb{R}^n \to \mathbb{R}^n$ defined by a bilinear multiplication b by equality $L_x(y) = b(x,y)$ is a linear endomorphism. Moreover, the mapping

$$L : \mathbb{R}^n \ni x \mapsto L_x \in \mathrm{End}(\mathbb{R}^n)$$

is a homomorphism of these linear spaces.

Similary,

$$R : \mathbb{R}^n \ni x \mapsto R_x \in \mathrm{End}(\mathbb{R}^n)$$

is a homomorphism ($R_x(y) = b(y,x)$). Conversely, every homomorphism

$$l : \mathbb{R}^n \to \mathrm{End}(\mathbb{R}^n)$$

defines a bilinear multiplication b_l by the formula:

$$b_l(x,y) = l(x)(y).$$

Then the left multiplication L of b_l is equal to l. A bilinear multiplication b has a left neutral element $\mathbb{1}_L \in \mathbb{R}^n$ if and only if

$$I \in L(\mathbb{R}^n) = (\text{the image of } L : \mathbb{R}^n \to \mathrm{End}(\mathbb{R}^n)).$$

Since $L(\mathbb{R}^n)$ is an n-dimensional linear subspace of the n^2-dimensional space $\mathrm{End}(\mathbb{R}^n)$, we can say that most of bilinear multiplications have no left neutral element. This is the generic case, i.e., such multiplications form an open and dense subset in the space $\mathrm{Hom}(\mathbb{R}^n, \mathrm{End}(\mathbb{R}^n))$ of bilinear multiplications. The same situation holds for multiplications without any right neutral element.

It is clear that the set of left neutral elements

$$\{x \in \mathbb{R}^n : b(x,y) = y \text{ for every } y \in \mathbb{R}^n\}$$

is equal to $\{x \in \mathbb{R}^n : L_x = I\}$, and therefore, it is either empty or it is a k-dimensional affine subspace in $\mathbb{R}^n$ equal to $\mathbb{1}_L + \ker L$, and $k = \dim(\ker L)$. Similarly, if there exists a right neutral element, say $\mathbb{1}_R \in \mathbb{R}^n$, then the set of all right neutral elements is equal to $\mathbb{1}_R + \ker R$, and it is also an affine subspace in $\mathbb{R}^n$. Elements of $\ker L$ are called left anihilators, since if $x \in \ker L$ then $b(x,y) = 0$ for every $y \in \mathbb{R}^n$. Analogously, elements of $\ker R$ are called right anihilators.

Since the group $\mathrm{Gl}(n,\mathbb{R})$ of linear isomorphisms of $\mathbb{R}^n$ acts transitively on $\mathbb{R}^n \setminus \{0\}$ (Cramer formulae), we see that every bilinear multiplication with a left (or right) neutral element (is isomorphic to a bilinear multiplication b with $e_1 = (1, 0, \ldots, 0)$ as one of its left (respectively, right) neutral elements. Let $\{e_1, \ldots, e_n\}$ be the standard basis of $\mathbb{R}^n$. Put

$$A_i = L_{e_i}, \quad i = 1, \ldots, n$$

and $\bar{A}_i$ is the matrix of endomorphism A_i in the basis $\{e_1, \ldots, e_n\}$.

Proposition 4.3. *The vector e_1 is the unit-element of a bilinear multiplication b if and only if the above defined matrices $\bar{A}_i$, $i = 1, \ldots, n$, have the form:*

$$\bar{A}_i = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \quad \text{and} \quad \bar{A}_i = \begin{bmatrix} 0, & b^i_{12} \ldots b^i_{1n} \\ \vdots & \\ 1, & b^i_{i2} \ldots b^i_{in} \\ \vdots & \\ 0, & b^i_{n2} \ldots b^i_{nn} \end{bmatrix} \quad \text{for } i \geq 2.$$

If $\bar{A}_1 = \begin{bmatrix} 1 & b^1_{12} \ldots b^1_{1n} \\ 0 & \\ \vdots & \\ 0 & b^1_{n2} \ldots b^1_{nn} \end{bmatrix}$ *and $\bar{A}_i$ for $i \geq 2$ are as above then e_1 is a right neutral element. If $\bar{A}_1 = I$ and $\bar{A}_i$ are arbitrary for $i \geq 2$ then e_1 is a left neutral element.*

Corollary 4.4. *The set of all bilinear multiplications that have a fixed $x_0 \in \mathbb{R}^n \setminus \{0\}$ as a left neutral element is an affine subspace of dimension $n^3 - n^2$. The analogous result holds if x_0 is a right neutral element. The set of all bilinear multiplications that have a fixed $x_0 \in \mathbb{R}^n - \{0\}$ as a unit-element is an affine subspace of dimension $n(n-1)^2$.*

This corollary follows easily from Proposition 4.3, if we look on the (linear) space of bilinear multiplications as on the product $(\mathrm{End}(\mathbb{R}^n))^n$, where the isomorphism

$$\mathrm{Hom}(\mathbb{R}^n, \mathrm{End}(\mathbb{R}^n)) \to (\mathrm{End}(\mathbb{R}^n))^n$$

is defined by $L \mapsto (A_1, \dots, A_n)$ as above.

If a multiplication $*$ in a basis $\mathcal{Z}$ of $\mathbb{R}^n$ has a left (or right) neutral element then this element is a left (respectively, right) neutral element of the induced bilinear multiplication $\times$ in $\mathbb{R}^n$. Also, if $z_1, \dots, z_k$ are left (or right) neutral element of $*$ then $\sum_{i=1}^k \lambda_i z_i$, where $\sum_{i=1}^k \lambda_i = 1$, is a left (respectively; right) neutral element of induced multiplication $\times$. But if the induced multiplication $\times$ by $*$ in $\mathcal{Z}$ has a left neutral element (respectively, right) then $*$ need not have any neutral element.

Example 4.5. Let $\{e_1, e_2, e_3\}$ be a basis of $\mathbb{R}^3$ and a multiplication $*$ is defined by the following table.

$*$	e_1	e_2	e_3
e_1	e_1	e_2	e_2
e_2	e_3	e_3	e_3
e_3	e_3	e_3	e_2

Then $*$ has neither a left nor a right neutral element. Nevertheless, the induced bilinear multiplication $\times$ in $\mathbb{R}^3$ by $*$ does have a left neutral element, namely,

$$\mathbb{1}_L = e_1 + e_2 - e_3$$

is the unique left neutral element of $\times$ what can easily be verified by solving the system of equations

$$(\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3) \times e_j = e_j, \qquad j = 1, 2, 3,$$

which has the form

$$\begin{cases} \lambda_1 = 1, & \lambda_2 + \lambda_3 = 0 \quad (j = 1), \\ \lambda_1 = 1, & \lambda_2 + \lambda_3 = 0 \quad (j = 2), \\ \lambda_1 + \lambda_3 = 0, & \lambda_2 = 1 \qquad\quad (j = 3). \end{cases}$$

For $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$ in $\mathbb{R}^3$, we obtain

$$(x_1, x_2, x_3) \times (y_1, y_2, y_3) = (x_1y_1, x_1y_2 + (x_1 + x_3)y_3, x_2(y_1 + y_2 + y_3) + x_3(y_1 + y_2)).$$

If we take the conjugated multiplication $\bar{*}$ then this multiplication induces the conjugated multiplication $\bar{\times}$ in $\mathbb{R}^3$ which has the unique right neutral element $e_1 + e_2 - e_3$, while $\bar{*}$ has no right neutral element.

We cannot also expect that a multiplication $*$ in $\mathcal{Z}$ has a unit-element, if the induced by $*$ bilinear multiplication $\times$ in $\mathbb{R}^n$ does have a unit element. Consider another multiplication $\triangle$ in the basis $\{e_1, e_2, e_3\}$ in $\mathbb{R}^3$ defined by the table

$\triangle$	e_1	e_2	e_3
e_1	e_1	e_3	e_3
e_2	e_3	e_2	e_3
e_3	e_3	e_3	e_3

Then $x = e_1 + e_2 - e_3$ is the unit-element of induced multiplication $\widetilde{\times}$ by $\triangle$, while $\triangle$ has no any neutral element (neither right nor left).

$$(x_1, x_2, x_3) \,\widetilde{\times}\, (y_1, y_2, y_3) = (x_1y_1, x_2y_2, (x_2 + x_3)y_1 + (x_1 + x_3)y_2 + (x_1 + x_2 + x_3)y_3).$$

Then $x_0 = (1, 1, -1)$ is the unit-element of $\widetilde{\times}$.

Proposition 4.6. *Let $\mathcal{Z} = \{z_1, \ldots, z_n\} \subset \mathbb{R}^n$ be a basis in $\mathbb{R}^n$ and $* : \mathcal{Z} \times \mathcal{Z} \to \mathcal{Z}$ is a multiplication such that every left multiplication L_{z_i} and every right multiplication R_{z_j} in $\mathcal{Z}$ are bijections. Then the induced bilinear multiplication $\times$ in $\mathbb{R}^n$ by $*$ has a left neutral element if and only if $*$ has a (unique) left neutral-element. The multiplication $\times$ in $\mathbb{R}^n$ has a right neutral element if and only if $*$ has a right neutral element. The multiplication $\times$ has the unit-element in $\mathbb{R}^n$ if and only if $*$ has unit-element in $\mathcal{Z}$ and this element of $\mathbb{R}^n$ is the common unit-element of both multiplications. Then $(\mathcal{Z}, *)$ is a quasigroup.*

Proof. The element $x = \sum_{i=1}^{n} \nu_i z_i$, $\nu_i \in \mathbb{R}$, is a left neutral element of $\times$ if and only if for every $j \in \{1, \ldots, n\}$ we have

$$\sum_{i=1}^{n} \nu_i (z_i * z_j) = z_j.$$

Since R_{z_j} is a bijection in $\mathcal{Z}$ and $\mathcal{Z}$ is a basis in $\mathbb{R}^n$, we see that there exists exactly one $l \in \{1, \ldots, n\}$ such that $z_l * z_j = z_j$ and for $k, p \in \{1, \ldots, n\}$ such that $l \neq k \neq p \neq l$ the following inequalities hold

$$z_j \neq z_k * z_j \neq z_p * z_j \neq z_j,$$

and thus,

$$\nu_l = 1 \quad \text{and} \quad \nu_i = 0 \quad \text{for } i \neq l.$$

For $j' \in \{1, \ldots, n\}$ and $j' \neq j$ we also obtain l' such that $z_{l'} * z_{j'} = z_{j'}$ and $\nu_{l'} = 1$, $\nu_i = 0$ for $i \neq l'$. Therefore $l' = l$ and $x = z_l$ is a left neutral element of $*$.

If $\times$ has a right neutral element, then this element is a left neutral element of the conjugated multiplication $\bar{\times}$ which is the bilinear multiplication induced by the conjugated multiplication $\bar{*}$. Therefore, $\bar{*}$ has unique left neutral element in $\mathcal{Z}$ which is a right neutral element of $*$.

Composing two above proven results we infer that if $\times$ has unit element then $(\mathcal{Z}, *)$ is a quasigroup and its unique unit-element is the unit-element of $(\mathbb{R}^n, \times)$. □

In the examples provided below we present matrices $\bar{A}_i$, $i = 1, \ldots, n$ in the standard basis of $\mathbb{R}^n$.

4.7. Examples

(i) $n = 2$. The multiplication in $\mathbb{R}^2$ is defined as usual complex numbers multiplication. Then it is a commutative, associative bilinear multiplication with unit-element $(1, 0)$ and $\bar{A}_1 = \begin{bmatrix} 1, & 0 \\ 0, & 1 \end{bmatrix}$, $\bar{A}_2 = \begin{bmatrix} 0, & -1 \\ 1, & 0 \end{bmatrix}$. The space $\mathbb{R}^2$ with addition and this multiplication is a field $\mathbb{C}$.

(ii) $n = 4$. Consider the multiplication of quaternions. Then

$$\bar{A}_1 = I, \quad \bar{A}_2 = \begin{bmatrix} 0, & -1, & 0, & 0 \\ 1, & 0, & 0, & 0 \\ 0, & 0, & 0, & -1 \\ 0, & 0, & 1, & 0 \end{bmatrix},$$

$$\bar{A}_3 = \begin{bmatrix} 0, & 0, & -1, & 0 \\ 0, & 0, & 0, & 1 \\ 1, & 0, & 0, & 0 \\ 0, & -1, & 0, & 0 \end{bmatrix}, \quad \bar{A}_4 = \begin{bmatrix} 0, & 0, & 0, & -1 \\ 0, & 0, & -1, & 0 \\ 0, & 1, & 0, & 0 \\ 1, & 0, & 0, & 0 \end{bmatrix}.$$

The space $\mathbb{R}^n$ with usual addition and the multiplication defined by the above matrices is the Hamilton's Algebra of quaternions (a non-commutative ring with unit-element such that every non-zero element is invertible, i.e., a skew field).

(iii) $n = 3$. $(a, b, c) \circ (x, y, z) := (ax, ay + bx, az + cx)$.
The multiplication $\circ$ in $\mathbb{R}^3$ is a commutative, associative, bilinear multiplication with unit-element $(1, 0, 0)$. Every element $(a, b, c) \in \mathbb{R}^3$ such that $a \neq 0$ is invertible

$$(a, b, c)^{-1} = \left(\frac{1}{a}, \frac{-b}{a^2}, \frac{-c}{a^2}\right) = \frac{-1}{a^2}(-a, b, c),$$

and for every $(b, c) \in \mathbb{R}^2$ the element $(0, b, c) \in \mathbb{R}^3$ has not inverse element. For $\circ$ we have

$$\bar{A}_1 = I, \quad \bar{A}_2 = \begin{bmatrix} 0, & 0, & 0 \\ 1, & 0, & 0 \\ 0, & 0, & 0 \end{bmatrix}, \quad \bar{A}_3 = \begin{bmatrix} 0, & 0, & 0 \\ 0, & 0, & 0 \\ 1, & 0, & 0 \end{bmatrix}.$$

(iv) $n = 3$. $(a, b, c) \triangle (x, y, z) := (ax, ay + bx + cy, az + cx)$.

The multiplication $\triangle$ in $\mathbb{R}^3$ is bilinear, non-commutative and non-associative, but it has unit-element, namely, $(1, 0, 0)$. Non-associativity of $\triangle$ follows from two equalities below.

$$\begin{aligned} [(0,0,1) \triangle (0,0,1)] \triangle (0,1,0) &= (0,0,0), \\ (0,0,1) \triangle [(0,0,1) \triangle (0,1,0)] &= (0,1,0). \end{aligned}$$

Since

$$(0,0,1) \triangle (0,1,0) = (0,1,0) \neq (0,0,0) = (0,1,0) \triangle (0,0,1),$$

we see that the multiplication $\triangle$ is not commutative. For $\triangle$ we obtain

$$\bar{A}_1 = I, \quad \bar{A}_2 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \bar{A}_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

(v) The vector product $\times$ in $\mathbb{R}^3$ is a skew-symmetric, non-associative, bilinear multiplication. It has no any neutral element as every skew-symmetric multiplication. We have here

$$\bar{A}_1 = \begin{bmatrix} 0, & 0, & 0 \\ 0, & 0, & -1 \\ 0, & 1, & 0 \end{bmatrix}, \quad \bar{A}_2 = \begin{bmatrix} 0, & 0, & 1 \\ 0, & 0, & 0 \\ -1, & 0, & 0 \end{bmatrix}$$
$$\text{and } \bar{A}_3 = \begin{bmatrix} 0, & -1, & 0 \\ 1, & 0, & 0 \\ 0, & 0, & 0 \end{bmatrix}.$$

(vi) Let $\mathcal{Z} = \{e_1, \dots, e_n\}$ be the standard basis in $\mathbb{R}^n$ and $*$ is any multiplication in $\mathcal{Z}$. Then the induced bilinear multiplication $\times$ in $\mathbb{R}^n$ has matrix $\bar{A}_i$, $i \in \{1, \dots, n\}$ such that if $e_i * e_j = e_k$ then there is only one non-zero element in j-th column of $\bar{A}_i$. It is equal to 1 and stands in k-th row. In particular, the bilinear multiplication $\square$ in $\mathbb{R}^2$,

$$(a, b) \,\square\, (x, y) = (ax + by, ay + bx)$$

is induced in the standard basis $\{e_1, e_2\}$, $e_1 = (1, 0), e_2 = (0, 1)$ by the multiplication $* = \Leftrightarrow$

$*$	e_1	e_2
e_1	e_1	e_2
e_2	e_2	e_1

The multiplication $\square$ is commutative, associative and $e_1 = (1, 0)$ is the unit-element of $\square$. We have

$$\bar{A}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \bar{A}_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

If $(a, b) \in \mathbb{R}^2$ and $a^2 - b^2 \neq 0$ then (a, b) is invertible and

$$(a, b)^{-1} = (a^2 - b^2)^{-1}(a, -b).$$

If $a^2 - b^2 = 0$ then (a, b) has no any inverse element. Since

$$(ax + by)^2 - (ay + bx)^2 = (a^2 - b^2)(x^2 - y^2),$$

we see that $\square$ when restricted to $Y \times Y$, where

$$Y = \{(a, b) \in \mathbb{R}^2 : a^2 - b^2 \neq 0\},$$

maps $Y \times Y \to Y$ and is a commutative group multiplication in Y.

This multiplication is also well defined in $Y \cap \mathbb{Z}^2$. But $(k, 0) \in Y \cap \mathbb{Z}^2$ is invertible if and only if $k = 1$ or $k = -1$. Therefore, $(Y \cap \mathbb{Z}^2, \square)$ is a semigroup. Anyway, Y has proper subgroups. The smallest one is $\{(+1, 0), (-1, 0)\}$. Next, $\mathbb{R}_+ \times \{0\}$ and $(\mathbb{R} \setminus \{0\}) \times \{0\}$ are also proper subgroups of $(Y, \square)$ and $\square$ restricted to $(\mathbb{R}_+ \times \{0\})^2$ or $((\mathbb{R} \setminus \{0\} \times \{0\})^2$ becomes the usual multiplication of real numbers (embedded in $\mathbb{C}$, $x \sim (x, 0)$) $Y_+ = \{(a, b) \in \mathbb{R}^2 : a^2 - b^2 > 0\}$ is also a subgroup, since $(ax + by)^2 - (ay + bx)^2 = (a^2 - b^2)(x^2 - y^2) > 0$ if $a^2 - b^2 > 0$ and $x^2 - y^2 > 0$, and $(a, b)^{-1} \in Y_+$ if $(a, b) \in Y_+$. Y_+ is a maximal proper subgroup of Y. Finally,

$$Y_0 = \{(a, b) \in \mathbb{R}^2 : a > |b|\},$$

i.e., the connective component of Y_+ containing neutral element $e_1 = (1, 0)$ in the Lie group $(Y, \square)$, is a proper subgroup. We have

$$ax + by - |ay + bx| = \begin{cases} (a-b)(x-y) & \text{if } ay + bx \geq 0, \\ (a+b)(x+y) & \text{if } ay + bx < 0. \end{cases}$$

Therefore, if $a > |b|$ and $x > |y|$ then

$$ax + by - |ay + bx| > (a - |b|)(x - |y|) > 0,$$

and thus $(a, b) \square (x, y) \in Y_0$ if $(a, b) \in Y_0$, if $a > |b|$. Also $(a, b)^{-1} \in Y_0$ if $(a, b) \in Y_0$:

$$\frac{a}{a^2 - b^2} - \left| \frac{-b}{a^2 - b^2} \right| = \frac{a - |b|}{a^2 - b^2} > 0, \quad \text{if } a > |b|.$$

The multiplication $\square$ may also be restricted to $\widetilde{Y} \times \widetilde{Y}$, where $\widetilde{Y} := \{(a, b) \in \mathbb{R}^2 : a > b\}$, since

$$(ax + by) - (ay + bx) = (a - b)(x - y) > 0,$$

if $a - b > 0$ and $x - y > 0$. But $(0, -1)$ has no inverse in $\widetilde{Y}$, since $(0, -1)^{-1} = (0, 1)$ (in Y) and $(0, 1) \notin \widetilde{Y}$. Thus, $(\widetilde{Y}, \square)$ is a semigroup. The space $(\mathbb{R}^2, +, \square)$ is not a field, but it is a commutative ring with unit-element.

In the forthcoming lemma we demonstrate a useful method of proving that a given multiplication is not induced by a multiplication in any basis of $\mathbb{R}^n$.

Lemma 4.8. *The multiplication $\circ$ in $\mathbb{R}^3$ defined in Examples 4.6 (iii) is not induced by any multiplication in any basis of $\mathbb{R}^3$.*

Proof. Let $\mathcal{Z} = \{z_1, z_2, z_3\}$ be any basis of $\mathbb{R}^3$ and $* : \mathcal{Z} \times \mathcal{Z} \to \mathcal{Z}$ is a multiplication. For the induced multiplication $\times$ in $\mathbb{R}^3$ by $*$ we have $z_i \times z_j \in \mathcal{Z}$ for every $i, j \in \{1, 2, 3\}$. In particular, for every $\zeta \in \mathcal{Z}$ we have $\zeta^2 = \zeta \times \zeta \in \mathcal{Z}$, $(\zeta^2)^2 \in \mathcal{Z}$, $[(\zeta^2)^2]^2 \in \mathcal{Z}, \ldots$. Define the sequence $(\xi_i)_{i \in \mathbb{N}}$ as follows. $\xi_1 := \zeta$, $\xi_{i+1} := \xi_i \times \xi_i$ for every $i \in \mathbb{N}$. If $\zeta \in \mathcal{Z}$ then for every $i \in \mathbb{N}$ the element ξ_i belongs to $\mathcal{Z}$, i.e., the sequence $(\xi_i)_{i \in \mathbb{N}}$ has finite set of all its values contained in $\mathcal{Z}$. Let us find now for the multiplication $\circ$ in $\mathbb{R}^3$ all points $\zeta \in \mathbb{R}^3$ such that the corresponding sequence $(\xi_i)_{i \in \mathbb{N}}$ (as above) has all values in a finite subset of $\mathbb{R}^3 \setminus \{(0, 0, 0)\}$. We see that for $\zeta = (x, y, z) \in \mathbb{R}^3$

$$\begin{aligned} &\xi_2 = \zeta^2 = (x, y, z)^2 = (x, y, z) \circ (x, y, z) = (x^2, 2xy, 2xz), \\ &\xi_3 = (\zeta^2)^2 = (x^4, 4x^3 y, 4x^3 z), \\ &\xi_4 = [(\zeta^2)^2]^2 = (x^8, 8x^7 y, 8x^7 z). \end{aligned}$$

If the first component x of ζ is different than $0, 1$ or -1, then x, x^2, x^4 and x^8 are four different numbers and thus $\{\xi_1, \xi_2, \xi_3, \xi_4\}$ is a 4-element set in $\mathbb{R}^3$. Hence, it is not a basis. Therefore, if ζ is an element of basis $\mathcal{Z}$ in $\mathbb{R}^3$ for which there exists a multiplication $*$ that induces $\circ$ then $x = 0$ or $x = 1$ or $x = -1$. We also see that

$$\xi_{i+1} = (x^{2^i}, 2^i x^{2^i-1} y, 2^i x^{2^i-1} z), \qquad i \in \mathbb{N}.$$

If $\zeta = (0, y, z)$ then $\zeta^2 = (0, 0, 0)$ is not an element of any basis $\mathcal{Z}$ of $\mathbb{R}^3$. If $x = 1$ then $\xi_1 = (1, y, z)$ and $\xi_{i+1} = (1, 2^i y, 2^i z)$. Therefore, $(\xi_i)_{i\in\mathbb{N}}$ has finite set of values if and only if $y = 0$ and $z = 0$. If $x = -1$ then $\widetilde{\xi}_1 = (-1, y, z)$, $\widetilde{\xi}_{i+1} = (1, -2^i y, -2^i z)$, and the sequence $(\widetilde{\xi}_i)_{i\in\mathbb{N}}$ has finite set of values if and only if $\widetilde{\xi}_1 = (-1, 0, 0)$. Since

$$\{(1, 0, 0), (-1, 0, 0)\}$$

is not a basis in $\mathbb{R}^3$ and $\zeta = (1, 0, 0)$, $\widetilde{\zeta} = (-1, 0, 0)$ are the only two points in $\mathbb{R}^3$ such that the sequences $(\xi_i)_{i\in\mathbb{N}}$ and $(\widetilde{\xi}_i)_{i\in\mathbb{N}}$ generated by ζ and $\widetilde{\zeta}$, respectively, have finite sets of values in $\mathbb{R}^3 \setminus \{(0, 0, 0)\}$, we infer that the multiplication $\circ$ is not induced by any multiplication $*$ in any basis $\mathcal{Z}$ of $\mathbb{R}^3$. □

We proved in Lemma 4.2 that the multiplication of complex numbers is not an induced multiplication in $\mathbb{R}^2$. The similar method or the method used to prove Lemma 4.8 can be applied to prove that quaternion multiplication in $\mathbb{R}^4$ also is not induced by any multiplication in a basis of $\mathbb{R}^4$. Also the vector product in $\mathbb{R}^3$ is not an induced multiplication, since $\zeta \times \zeta = (0, 0, 0)$ for every $\zeta \in \mathbb{R}^3$.

5. Why $\mathbb{R}^{2k+1}$, $k \in \mathbb{N}$, cannot be a Skew Field

A skew field is also called a division ring (see Cohn [1], p. 130) and it is a ring with unit-element such that every non-zero element in it is invertible. It is known that every finite skew field is commutative (the Witt's proof of this theorem proven in 1905 by Wedderburn can be found in Cohn [1], pp. 178, 179). The theory of finite fields is complete nowadays and its expositiory lecture can be found e.g. in Lidl, Niederreiter [3]. It is also well known that every complete normed skew field is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ if it is commutative or to $\mathbb{H}$ — the Hamilton's Algebra of quaternions, if it is non-commutative.

When $*$ is a commutative multiplication in a basis $\mathcal{Z}$ of $\mathbb{R}^n$ then the induced multiplication $\times$ in $\mathbb{R}^n$ is commutative. Also, if $*$ is an associative multiplication in $\mathcal{Z}$ then $\times$ is an associative multiplication in $\mathbb{R}^n$. Therefore, if $(\mathcal{Z}, *)$ is a group then $(\mathbb{R}^n, +, \times)$ is a ring with unit-element, since the neutral element of $*$ in $\mathcal{Z}$ is also the unit-element of $\times$ in $\mathbb{R}^n \supset \mathcal{Z}$. We proved in the previous paragraph that multiplications in $\mathbb{C}$ and $\mathbb{H}$ are not induced by any multiplication $*$ in any basis $\mathcal{Z}$ of $\mathbb{R}^2$ or $\mathbb{R}^4$, respectively. Hence, introducing in a basis $\mathcal{Z}$ of $\mathbb{R}^n$ a group structure (through a bijection of $\mathcal{Z}$ and a multiplicative group $K^\times = K \setminus \{0\}$ of a finite field K for $n = p^k - 1$, $k \in \mathbb{N}$, and p being a prime number in $\mathbb{N}$), we do not obtain a skew field structure on $\mathbb{R}^n$. For instance, if $K = \mathbb{F}_3 = \mathbb{Z}/3$ then the multiplication $*$ in the basis $\mathcal{Z} = \{e_1, e_2\}$ of $\mathbb{R}^2$ isomorphic to the multiplication of the multiplicative group $K^\times$ is as follows

$*$	e_1	e_2
e_1	e_1	e_2
e_2	e_2	e_1

and this multiplication induces the multiplication $\times = \square$ in $\mathbb{R}^2$ described in Example 4.6 (vi).

When we take the bijection $\psi : \mathbb{F}_2 \to \{e_1, e_2\}$, $\psi(1) = e_1$, $\psi(0) = e_2$, then this bijection defines in the basis $\mathcal{Z}$ the following multiplication $\triangledown$ isomorphic to the multiplication in $\mathbb{F}_2$

$\triangledown$	e_1	e_2
e_1	e_1	e_2
e_2	e_2	e_2

Then the multiplication $\times$ in $\mathbb{R}^2$ induced by $\triangledown$ is as follows

$$(a, b) \times (x, y) = (ax, ay + bx + by).$$

The vector e_1 is the unit-element od $\times$ and $\times$ is a commutative and associative multiplication of $\mathbb{R}^2$. But $(a, b) \in \mathbb{R}^2$ is invertible (with respect to $\times$) if and only if $a \neq 0$ and $a + b \neq 0$. Then

$$(a, b)^{-1} = \left(\frac{1}{a}, \frac{-b}{a(a+b)} \right).$$

Therefore, the ring $(\mathbb{R}^2, +, \times)$ with the unit-element $(1, 0)$ is not a division ring.

Now we provide here a very simple argument that answers the question in the title of this paragraph.

Proposition 5.1. *If $k \in \mathbb{N}$, $n = 2k + 1$, and $*$ is a bilinear multiplication in $\mathbb{R}^n$ then there exist $\zeta \in \mathbb{R}^n \setminus \{0\}$ and $\eta \in \mathbb{R}^n \setminus \{0\}$ such that $\zeta * \eta = 0$. Hence, for every such n and $*$ the space $(\mathbb{R}^n, +, *)$ is not a division ring.*

Proof. Obviously, $\zeta * \eta = 0$ if and only if $\eta \in \ker L_\zeta$. Thus, it is sufficient to find a $\zeta \in \mathbb{R}^{2k+1} \setminus \{0\}$ such that $\det L_\zeta = 0$. For $(i,j) \in \mathbb{N}^2$ such that $1 \le i \le n$ and $1 \le j \le n$ there exist numbers $a_{ij}^m \in \mathbb{R}$ such that the matrix of L_x in the standard basis $\{e_1, \dots, e_n\}$ of $\mathbb{R}^n$ has the number $\sum_{m=1}^n a_{ij}^m x_m$ on the (i,j)-th place for any $x = (x_1, \dots, x_n) \in \mathbb{R}^n$. In fact, the number a_{ij}^m stands in the i-th row and j-th column of the matrix $\overline{A_m}$ of L_{e_i} (in the standard basis). We see that

$$\det L_x = \sum_{m=1}^n x_m \begin{vmatrix} a_{11}^m, & \dots, & a_{1j}^m, & \dots, & a_{1n}^m \\ \vdots & & \vdots & & \vdots \\ \sum_{l=1}^n a_{i1}^l x_l, & \dots, & \sum_{l=1}^n a_{ij}^l x_l, & \dots, & \sum_{l=1}^n a_{in}^l x_l \\ \vdots & & \vdots & & \vdots \\ \sum_{l=1}^n a_{n1}^l x_l, & \dots, & \sum_{l=1}^n a_{nj}^l x_l, & \dots, & \sum_{l=1}^n a_{nn}^l x_l \end{vmatrix},$$

for $i \ge 2$. Applying the additivity rule for the other $2k$ rows of the n determinants appearing in this sum, we finally find that

$$\det L_x = a(x_{2k+1})^{2k+1} + \sum_{j=1}^{2k+1} (x_{2k+1})^{2k+1-j} P_j(x_1, \dots, x_{2k}),$$

where

$$a = \begin{vmatrix} a_{11}^n & \dots & a_{1n}^n \\ a_{n1}^n & \dots & a_{nn} \end{vmatrix}, \qquad n = 2k+1,$$

and every P_j is a homogeneous polynomial of order j in $2k$ variables $x_1, x_2, \dots, x_{2k}$. If $a = 0$ then $x = \zeta = (0, \dots, 0, 1)$ satisfies the equality $\det L_x = 0$.

If $a \neq 0$ then

$$\det L_{(1,0,\dots,0,t)} = at^{2k+1} + \sum_{j=1}^{2k+1} p_j t^{2k+1-j},$$

where $p_j = P_j(1, 0, \dots, 0)$, is a polynomial of the odd order $2k+1$. Hence, this polynomial has at least one real root t_0. Therefore, for $\zeta = (1, 0, \dots, 0, t_0)$ we have $\det L_\zeta = 0$. Thus, there exists $\eta \in \mathbb{R}^n \setminus \{0\}$ such that $\zeta * \eta = 0$. If the triple $(\mathbb{R}^n, +, *)$ were a skew field then for $\zeta = (1, 0, \dots, 0, t_0)$ and $\eta \in (\ker L_\zeta \setminus \{0\})$ we would have

$$0 = 0 * \eta^{-1} = (\zeta * \eta) * \eta^{-1} = \zeta * (\eta * \eta^{-1}) = \zeta * \mathbb{1} = \zeta$$

whict contradicts $\zeta \neq 0$. This concludes the proof. □

The elements ζ and η as in Proposition 5.1 are called zero-divisors. In other words, this Proposition says that every $(\mathbb{R}^{2k+1}, +, *)$, $k \in \mathbb{N}$, has zero-divisors if $*$ is bilinear, even if it is not associative, that is, $(\mathbb{R}^{2k+1}, +, *)$ need not be a ring in a commonly used sense.

References

[1] P.M. Cohn, *Basic Algebra, Groups, Rings and Fields*, Springer (2003).

[2] H. Kurzweil, B. Stellmacher, *The Theory of Finite Groups*, Springer (2004).

[3] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, **20**, MIT, Cambridge, Massachusetts (1983).

[4] A. Lubotzky, D. Segal, *Subgroup Growth*, Progress in Mathematics, Volume **212**, Birkhäuser (2003).

[5] A. Seress, *Permutation Group Algorithms*, Cambridge University Press (2002).